09/856613

SD

11/04/2004

1. A method of protecting data in a system including a microprocessor (106) having at least one hardware break point (301), characterized in that it includes an operation of allocating a break point to data to be protected, in that it consists of instigating in said microprocessor (106) the generation of a break or interrupt (301) each time one of said protected data is accessed.

2. A protection method according to claim 1, characterized in that it includes an access validity verification operation (302, 303) at each break (301) triggered by a hardware break point allocated to protected data.

3. (Amended) A protection method according to claim 1, characterized in that it includes an operation (302) of verifying the programming of the control registers at each break (301) triggered by a hardware break point allocated to protected data.

4. (Amended) A protection method according to claim 1, characterized in that it includes an operation (303) of verifying that the interrupt return address is in the authorized area of the program at each break (301) triggered by a hardware break point allocated to protected data.

5. (Amended) A protection method according to claim 2, characterized in that it includes an operation (305) of invoking an error manager if at least one verification operation (302, 303) gives a negative result.

6. A device for protecting data in a system including a microprocessor (106) having at least one hardware break point, characterized in that it includes means (106) for allocating a break point to data to be protected.

7. A protection device according to claim 6, characterized in that it includes means (106) for verifying the validity of each access corresponding to a break triggered by a hardware break point allocated to protected data.

8. (Amended) A protection device according to claim 6, characterized in that it includes means (106) for verifying the programming of the control registers.

9. (Amended) A protection device according to claim 6, characterized in that it includes means (106) for verifying that the interrupt return address is in the authorized area of the program.

10. (Amended) A protection device according to claim 6, characterized in that it includes means (106) for invoking an error manager if at least one verification means supplies a negative verification result.

--11. (New) A protection method according to claim 2, characterized in that it includes an operation (302) of verifying the programming of the control registers at each break (301) triggered by a hardware break point allocated to protected data.

12. (New) A protection method according to claim 2, characterized in that it includes an operation (303) of verifying that the interrupt return address is in the authorized area of the program at each break (301) triggered by a hardware break point allocated to protected data.

13. (New) A protection method according to claim 3, characterized in that it includes an operation (303) of verifying that the interrupt return address is in the authorized area of the program at each break (301) triggered by a hardware break point allocated to protected data.

14. (New) A protection method according to claim 3, characterized in that it includes an operation (305) of invoking an error manager if at least one verification operation (302, 303) gives a negative result.

15. (New) A protection method according to claim 4, characterized in that it includes an operation (305) of invoking an error manager if at least one verification operation (302, 303) gives a negative result.

16. (New) A protection device according to claim 7, characterized in that it includes means (106) for verifying the programming of the control registers.

17. (New) A protection device according to claim 7, characterized in that it includes means (106) for verifying that the interrupt return address is in the authorized area of the program.

18. (New) A protection device according to claim 8, characterized in that it includes means (106) for verifying that the interrupt return address is in the authorized area of the program.

20. (Amended) A protection device according to claim 8, characterized in that it includes means (106) for invoking an error manager if at least one verification means supplies a negative verification result.

21. (Amended) A protection device according to claim 9, characterized in that it includes means (106) for invoking an error manager if at least one verification means supplies a negative verification result.--